UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/780,681	02/08/2001	Thomas A. Kean	19546-020200US	8254

7590 08/17/2004

Donald Daybell, Esq.
ORRICK, HERRINGTON & SUTCLIFE LLP
4 Park Plaza
Suite 1600
Irvine, CA 92614-2558

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	13

DATE MAILED: 08/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/780,681	KEAN, THOMAS A.	
	Examiner	Art Unit	
	Linh Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 February 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4,5*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Regarding claim 8, the phrase "about" renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d). Appropriate Correction is necessary.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3, 5, 9, 11-13, 16, 25-27, 29, 33, 35, 37, and 41 are rejected under 35 U.S.C. 102(e) as being anticipated by Erickson et al, US patent No. 6212639B1, hereinafter "Erickson".

5. As per claims 1 and 25, Erickson discloses the "Encryption of Configuration Stream" invention, which includes a method of encrypting data using the programmable logic device (PLD) utilizing keys generated by the security circuit (Col 4 lines 13-67) comprising: fabricating a first plurality of FPGA integrated circuits (Col 1 lines 15 to 57 and Col 3 lines 54-67) with a first secret key embedded by way of a first mask set (Col 4 lines 60-64); and fabricating a second plurality of FPGA integrated circuits with a second secret key embedded by way of a second mask set (Col 4 lines 60-64 and Col 7 lines 2-7).

6. As per claims 2 and 26, Erickson discloses the method of claims 1 and 25 wherein a first secure bit-stream will configure properly user-configurable logic of the first plurality of FPGA integrated circuits, but not the second plurality of FPGA integrated circuits (Col 5 lines 6-39).

7. As per claims 3 and 27, Erickson discloses the method of claims 1 and 25 further comprising: loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits to generate a secure bitstream using the first secret key (Col 5 lines 7-20).

8. As per claims 5, 9, 29, and 33, Erickson discloses the method of claims 1 and 25 wherein the first plurality of FPGA integrated circuits with the first secret key are fabricated in a first time period and the second plurality of FPGA integrated circuits with

the second secret key are fabricated in a second time period, different from the first time period (Col 5 lines 7-20).

9. As per claims 11 and 35, Erickson discloses the method of claims 1 and 25 wherein there are random differences between artwork of the first and second plurality of FPGA integrated circuits in addition to the different embedded secret keys (Col 4 lines 60-63, Col 5 line 27, lines 35-39, and line 45).

10. As per claims 12 and 36, Erickson discloses the method of claims 1 and 25 wherein the first and second secret keys are presented on wires of respective plurality of FPGA integrated circuits for only a limited duration (Col 5 lines 7-17).

11. As per claims 13 and 37, Erickson discloses the method of claims 1 and 25 wherein the first secret key is embedded by setting an initial state of a selection of memory cells in a device configuration memory of the FPGA integrated circuit (Col 7 lines 1-10).

12. As per claim 16, Claim 2 is incorporated. Further Erickson also teach the usage of an on-chip generated random number to encrypt the data (Col 4 lines 29-33).

13. As per claim 41, Erickson discloses the method of claim 25 further comprising: downloading a secure programmable integrated circuit bitstream through a network; and

configuring one of the first plurality of programmable integrated circuits using the secure programmable integrated circuit bitstream by decoding the secure programmable integrated circuit bitstream using the first secret key (Col 10 lines 20-45).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 4, 7, 8, 18-21, 28, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson.

16. As per claims 4 and 28, Erickson discloses the method of claims 1 and 28. However, Erickson does not teach the first plurality of FPGA integrated circuits with the first secret key are assigned to a first geographic area and the second plurality of FPGA integrated circuits with the second secret key are assigned to a second geographic area. Nevertheless, Erickson teaches the use of the key generation to connect privately to a received device for transferring encrypted data (Col 5 lines 20-39). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art to acknowledge that the same method can be used to distribute the encrypted data to different geographic area.

17. As per claims 7 and 31, Erickson discloses the method of claims 1 and 25. However Erickson does not teach the first plurality of FPGA integrated circuits with the first secret key are assigned exclusively to a first customer and the second key to a second customer. Nevertheless, Erickson does teach a key storage memory (Col 5 lines 10 to 11) and the configuration program logic (Col 3 lines 5-21). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art that Erickson invention does have capability to create exclusive rights for the usage of the key to a particular customer.

18. As per claims 8 and 32, Erickson discloses the method of claims 5 and 29. However, Erickson does not teach the first time period is about the same duration as the second time period directly. Nevertheless, Erickson does teach a capablily of programming the PLD to utilizing two keys at once (Col 5 lines 40-59). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art that the PLD can encrypt the bitstream at the same time period.

19. As per claim 18, Erickson discloses a method comprising: embedding a first secret key within the artwork of an FPGA integrated circuit (Col 5 lines 7-20); storing second secret key within an encrypted FPGA bitstream stored in an external nonvolatile memory accessible by the FPGA; decrypting the user-defined second secret key using the first secret key; and setting up a secure network link between the FPGA and a

server using the user-defined second secret key (PLD public key for secure connection) (Col 5 lines 20-57). However, Erickson does not teach the user can define the second key. Nevertheless, Erickson does teach the configurable logic elements which are programs to initialize the PLD to carry out tasks (Col 3 lines 23-50). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art to preprogram the PLD to use the second key to create a secure communication connection.

20. As per claims 19-21, Erickson discloses the method of claim 18 further comprising: downloading an FPGA bitstream using the secure network link; encrypting the downloaded FPGA bitstream using the first secret key; and storing the encrypted downloaded bitstream in the external memory (Col 5 lines 20-57 and Col 10 lines 3-45).

21. Claims 6, 10, 30 and 34, are rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson in view of Kean et al, US Patent No. 6292018B1, hereinafter "Kean".

22. As per claims 6 and 30, Erickson discloses the method of claims 1 and 25. However, Erickson does not teach the only one mask differs between the first and second mask sets. Nevertheless, Kean does teach the one mask differs between the first and the second mask sets (Col 30 lines 33-60). Therefore, it would be obvious at

the time of the invention was made for one of ordinary skill in the art to combine both teachings to switch the masking at a fast rate.

23. As per claims 10 and 34, Erickson discloses the method of claims 6 and 30. However, Erickson does not teach the one mask is a contact mask. Nevertheless, Kean does (Col 29 lines 2-11). Therefore, it would be obvious at the time of the invention was made for one of ordinary skill in the art to combine both teachings to switch the masking at a fast rate.

24. Claims 14-15, 17, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson in view of Plants, US Patent no. 6560743B2.

25. As per claims 14-15, and 38, Erickson discloses the method of claims 1 and 25. However, Erickson does not teach the first secret key is embedded by changes to a relatively large block of logic in the first plurality of FPGA integrated circuits and its value extracted using a CRC algorithm. Nevertheless, Plants discloses the "Cyclic Redundancy Checking of a Field Programmable Gate Array Having a SRAM Memory Architecture" invention, which has a CRC circuit to make sure the correct data is received (Col 2 lines 50-67 and Col 7 lines 8-16). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art to incorporate Plants CRC checking method into Erickson invention to add the data and key integrity checking mechanism.

26. As per claims 17, Erickson discloses the method of claim 1 further comprising: loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random number (Col 4 lines 28-39). However, Erickson does not teach the secure bitstream includes a message authentication code (MAC). Nevertheless, Plants does teach the implementation of the MAC or well know in the art the "signature" to check the validity of the data stream (Col 10 lines 65-67). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art to incorporate Plants CRC checking method into Erickson invention to add the data integrity checking mechanism.

27. Claims 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson in view of Candelore et al, US Patent no. 6061449, hereinafter "Candelore".

28. As per claim 22, Erickson discloses a method comprising: storing a first secret key on an FPGA chip (See Claim 18). However, Erickson does not teach the causing of the FPGA to calculate a message authentication code (MAC) corresponding to a user design; and storing the message authentication code with bitstream information in a nonvolatile memory. Nevertheless, Candelore discloses the "Secure Processor with External Memory Using Block Chaining and Block Re-ordering" invention, which includes the generation of the MAC and storage device for keeping necessary info to

receive the contents data and authentication data (Col 4 lines 45-64). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art to incorporate both teaching to ensure high quality data protection.

29. Claims 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson in view of Candelore, and further in view of Kocher et al, US Patent No. 2004011631 A1, hereinafter "Kocher".

30. As per claims 23 and 24, Erickson and Candelore disclose the method of claim 22 wherein the detecting unauthorized alterations to the bitstream using the message authentication code and storing the MAC in the storage device (Candelore, Col 4 lines 45-64). However Neither Erickson or Candelore teach the method further comprising: storing copyright messages with the bitstream information; and preventing bitstreams, which have been altered from being used to configure an FPGA. Nevertheless, Kocher does teach a method of using the FPGA to watermark the data stream with identity of the copyright owner. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to combine the teachings to create a secure content distribution service.

Conclusion

31. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914.

32. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.

Linh LD Son

Patent Examiner